UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/880,700	06/13/2001	Richard J. Takahashi	4224-19US1	4288

29974 7590 01/12/2005

GAMMAGE & BURNHAM, PLC
c/o PortfolioIP
P.O. BOX 52050
Minneapolis, MN 55402

EXAMINER	
PARTHASARATHY, PRAMILA	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 01/12/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/880,700	**Applicant(s)** TAKAHASHI, RICHARD J.	
	Examiner Pramila Parthasarathy	**Art Unit** 2136	

-- The MAILING DATE of this communication appears n the c ver sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 22 December 2004.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-33 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-33 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 09/03, 7/02 & 6/01.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on 12/22/2004. Claims 1 – 33 were received for consideration. No preliminary amendments to the claims were filed. Claims 1 – 33 are currently being considered.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1 – 33 are rejected under 35 U.S.C. 102(e) as being anticipated by Qi (US publication number 2002/0184498).

Regarding Claim 1, Qi teaches and describes a method for creating a message digest from a message, wherein a sequence of input words is derived from the message (Fig. 2 – 10; Summary and Page 3 paragraph [0029] – Page 6 paragraph [0075]), and the method comprises:

performing a first round during an iteration of the method, wherein the first round is a calculation that operates on a next word of the sequence (Page 3 paragraph [0031] – Page 4 paragraph [0042] and Page 5 paragraph [0048]);

performing a second round during the iteration of the method, wherein the second round is a calculation that operates on another next word of the sequence (Page 3 paragraph [0031] – Page 4 paragraph [0042] and Page 5 paragraph [0048]); and

repeating performing the first round and performing the second round until calculations have been performed that sequentially operate on all remaining words of the sequence (Page 5 paragraph [0058] – Page 6 paragraph [0069]).

Regarding Claim 11, Qi teaches and describes a computer readable medium having computer executable instructions stored thereon for performing a method for creating a message digest from a message, wherein a sequence of input words is derived from the message (Fig. 2 – 10; Summary and Page 3 paragraph [0029] – Page 6 paragraph [0075]), and the method comprises:

performing a first round during an iteration of the method, wherein the first round is a calculation that operates on a next word of the sequence (Page 3 paragraph [0031] – Page 4 paragraph [0042] and Page 5 paragraph [0048]);

performing a second round during the iteration of the method, wherein the second round is a calculation that operates on another next word of the sequence

(Page 3 paragraph [0031] – Page 4 paragraph [0042] and Page 5 paragraph [0048]); and

repeating performing the first round and performing the second round until calculations have been performed that sequentially operate on all remaining words of the sequence(Page 5 paragraph [0058] – Page 6 paragraph [0069]).

Regarding Claim 20, Qi teaches and describes an integrated circuit for creating a message digest from a message, wherein a sequence of input words is derived from the message (Fig. 2 – 10; Summary and Page 3 paragraph [0029] – Page 6 paragraph [0075]), and the integrated circuit comprises:

a first logic block which performs a first round during a pass through the first logic block, wherein the first round is a calculation that operates on a next word of the sequence (Page 3 paragraph [0031] – Page 4 paragraph [0042] and Page 5 paragraph [0048]); and

a second logic block, coupled to the first logic block, which performs a second round during a pass through the second logic block, wherein the second round is a calculation that operates on another next word of the sequence (Page 3 paragraph [0031] – Page 4 paragraph [0042] and Page 5 paragraph [0048]), and

wherein additional passes through the first logic block and the second logic block are made until calculations have been performed that sequentially operate on all remaining words of the sequence (Page 5 paragraph [0058] – Page 6 paragraph [0069]).

Regarding Claim 29, Qi teaches and describes an electronic device comprising:

an integrated circuit, which creates a message digest from a message, wherein a sequence of input words is derived from the message, and the message digest is created by performing a first round during an iteration of a one-way hash algorithm, wherein the first round is a calculation that operates on a next word of the sequence, and by performing a second round during the iteration of the method, wherein the second round is a calculation that operates on another next word of the sequence, and by repeating performing the first round and performing the second round until

calculations have been performed that sequentially operate on all remaining words of the sequence (Page 3 paragraph [0031] – Page 4 paragraph [0042] and Page 5 paragraph [0048] and (Page 5 paragraph [0058] – Page 6 paragraph [0069]).

Claims 2, 12 and 21 are rejected as applied above in rejecting Claims 1, 11 and 20. Furthermore, Qi teaches and describes a method for creating a message digest from a message (Fig. 2 – 10; Summary and Page 3 paragraph [0029] – Page 6 paragraph [0075]), wherein a sequence of input words is derived from the message, further comprising performing the first round and the second round during a single clock cycle (Page 2 paragraph [0015] and Page 3 paragraph [0031] – Page 4 paragraph [0039]).

Claims 3, 13 and 22 are rejected as applied above in rejecting Claims 1, 11 and 20. Furthermore, Qi teaches and describes a method for creating a message digest from a message (Fig. 2 – 10; Summary and Page 3 paragraph [0029] – Page 6 paragraph [0075]), wherein performing the first round comprises using at least one carry save adder and a first full adder (Page 5 paragraph [0048 – 0051] and Page 5 paragraph [0058] – Page 6 paragraph [0061]).

Claims 7, 17, 26 and 30 are rejected as applied above in rejecting Claims 1, 11, 20 and 29. Furthermore, Qi teaches and describes a method for creating a message digest from a message (Fig. 2 – 10; Summary and Page 3 paragraph [0029] – Page 6 paragraph [0075]), further comprising performing two or more additional rounds during the iteration (Page 5 paragraph [0058] – Page 6 paragraph [0068]).

Claim 8 is rejected as applied above in rejecting Claim 1. Furthermore, Qi teaches and describes a method for creating a message digest from a message (Fig. 2 – 10; Summary and Page 3 paragraph [0029] – Page 6 paragraph [0075]), further comprising performing a serial to parallel conversion process on a set of bits to create the next word, the another next word, and the all remaining words (Page 6 paragraph [0062 – 0075]).

Claim 9, 18 and 27 are rejected as applied above in rejecting Claims 1, 11 and 20. Furthermore, Qi teaches and describes a method for creating a message digest from a message (Fig. 2 – 10; Summary and Page 3 paragraph [0029] – Page 6 paragraph [0075]), wherein the message comprises one or more 512-bit blocks, each of which includes sixteen 32-bit words, and the message digest includes 160 bits (Page 4 paragraph [0038], [0044].

Claim 10, 19 and 28 are rejected as applied above in rejecting Claims 1, 11 and 20. Furthermore, Qi teaches and describes a method for creating a message digest from a message (Fig. 2 – 10; Summary and Page 3 paragraph [0029] – Page 6 paragraph [0075]), wherein the message digest is identical to another message digest computed by SHA-I, given a same message (Page 4 paragraph [0038], [0044] and [0045]).

Claim 31 is rejected as applied above in rejecting Claim 29. Furthermore, Qi teaches and describes a method for creating a message digest from a message (Fig. 2 – 10; Summary and Page 3 paragraph [0029] – Page 6 paragraph [0075]), wherein the integrated circuit comprises:

a first logic block, which performs the first round during a pass through the first logic block (Page 3 paragraph [0031] – Page 4 paragraph [0042] and Page 5 paragraph [0048]); and a second logic block, coupled to the first logic block, which performs the second round during a pass through the second logic block (Page 3 paragraph [0031] – Page 4 paragraph [0042] and Page 5 paragraph [0048]), and

wherein additional passes through the first logic block and the second logic block are made until calculations have been performed that sequentially operate on all remaining words of the sequence (Page 5 paragraph [0058] – Page 6 paragraph [0069]).

Claim 32 is rejected as applied above in rejecting Claim 29. Furthermore, Qi teaches and describes a method for creating a message digest from a message (Fig. 2 – 10; Summary and Page 3 paragraph [0029] – Page 6 paragraph [0075]), further comprising:

an external interface, which transmits the message digest (Fig. 1 and Page 2 paragraph [0028]).

Claim 33 is rejected as applied above in rejecting Claim 29. Furthermore, Qi teaches and describes a method for creating a message digest from a message (Fig. 2 – 10; Summary and Page 3 paragraph [0029] – Page 6 paragraph [0075]), further comprising:

an external interface, which transmits data that was generated from the message digest (Fig. 1 and Page 2 paragraph [0028]).

Claims 4, 14 and 23 are rejected as applied above in rejecting Claims 3, 13 and 22. Furthermore, Qi teaches and describes a method for creating a message digest from a message (Fig. 2 – 10; Summary and Page 3 paragraph [0029] – Page 6 paragraph [0075]), further comprising:

initializing a first set of registers to a predetermined set of initialization values; wherein performing the first round includes adding the next word of the sequence to modified and unmodified versions of at least some of the first set of registers using the at least one carry save adder; and incorporating, by the first 111 adder, a first carry produced by the at least one carry save adder (Page 3 paragraph [0031 – 0036]).

Claims 5, 15 and 24 are rejected as applied above in rejecting Claims 3, 13 and 22. Furthermore, Qi teaches and describes a method for creating a message digest from a message (Fig. 2 – 10; Summary and Page 3 paragraph [0029] – Page 6 paragraph [0075]), wherein performing the second round comprises using at least one additional carry save adder and a second full adder (Page 5 paragraph [0048] and Page 6 paragraph [0061 – 0068]).

Claims 6, 16 and 25 are rejected as applied above in rejecting Claims 1, 11 and 20. Furthermore, Qi teaches and describes a method for creating a message digest from a message (Fig. 2 – 10; Summary and Page 3 paragraph [0029] – Page 6 paragraph [0075]), wherein performing the second round comprises:

adding, by the at least one additional carry save adder, the another next word of the sequence to a modified version of an output of the first full adder, and to modified and unmodified versions of at least some of the first set of registers (Page 5 paragraph [0048 – 0059] and Page 6 paragraph [0061 – 0068]); and

incorporating, by the second full adder, a second carry produced by the at least one additional carry save adder (Page 5 paragraph [0048 – 0059] and Page 6 paragraph [0061 – 0068]).

Conclusion

3. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have any questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AU 2131
1/10/05

Pramila Parthasarathy
January 03, 2005.